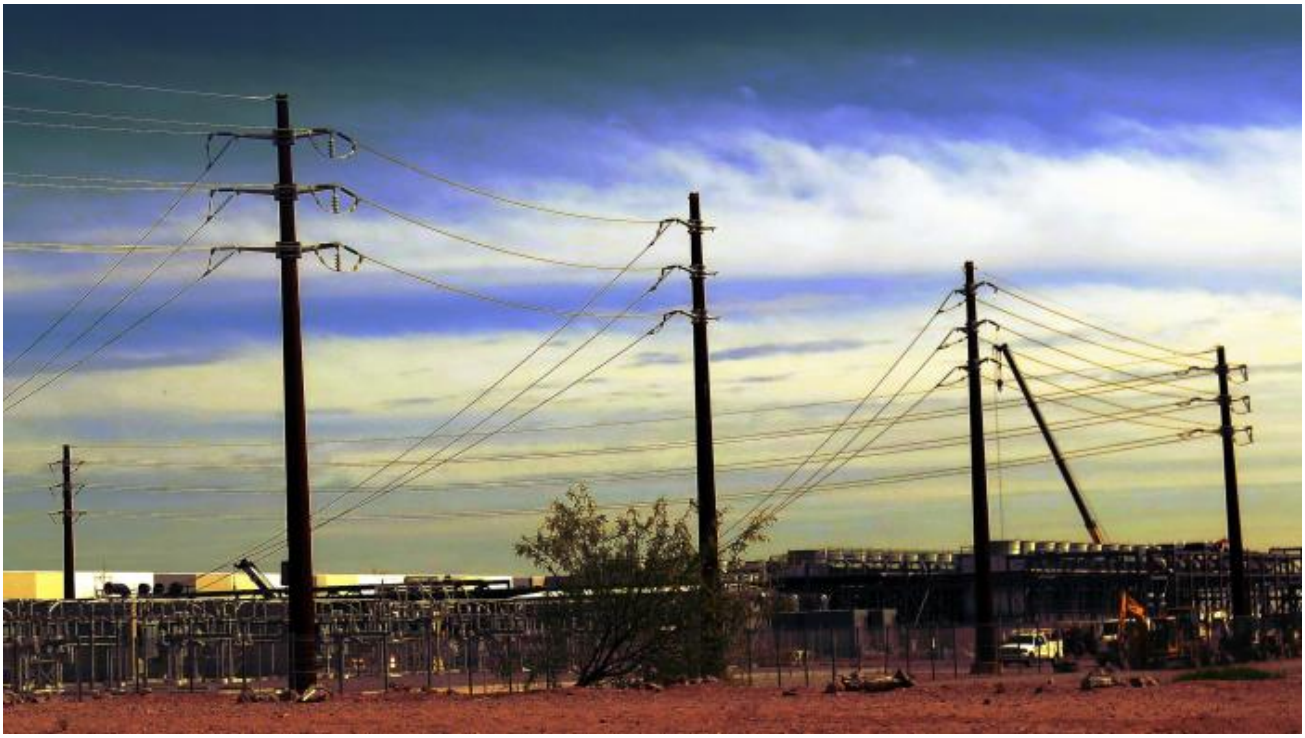
heise online

Botnetze können das Stromnetz sabotieren

26.12.2017 10:37 Uhr
Daniel AJ Sokolov



(Bild: Daniel AJ Sokolov)

Ein Botnetz könnte den Stromverbrauch vernetzter Geräte rascher beeinflussen, als Stromnetze darauf reagieren können. Damit könnte die Stromversorgung ganzer Länder sabotiert werden.

Wenige Millionen Computer, die koordiniert den Stromverbrauch erhöhen und senken, können Teile des kontinentaleuropäische Stromnetz zusammenbrechen lassen. Botnetze eigenen sich für solch eine Attacke also bestens. Sie können Computer und andere vernetzte Geräte schneller steuern, als das Stromnetz reagieren kann. So können Notabschaltungen oder auch physische Schäden an Netzeinrichtungen provoziert werden. Das zeigt eine Studie des österreichischen Forschungsinstituts SBA Research.

Die Steuerungstechnik der Stromnetze muss weder "smart" noch mit Sicherheitslücken behaftet sein. Die Botnetze greifen ja nicht direkt die Einrichtungen der Energieversorger an, sondern werden zur Steuerung am Stromnetz angeschlossener Verbraucher eingesetzt. Die Bots können beispielsweise Prozessoren und Grafikkarten unter Vollast laufen lassen oder in Stromsparmodus versetzen, die Helligkeit von Monitoren steuern oder Laserdrucker

anwerfen.

Außerdem kapern Bots immer häufiger Geräte wie "smarte" Fernseher oder vernetzte Thermostate, Haushaltsgeräte und andere Apparate des Internet of Things (IoT). Damit könnte ein Angreifer noch erheblich größere Schwankungen im Stromverbrauch erzeugen. Dabei muss er gar keine Überlastung der Stromleitung erreichen. Es reichte schon aus, den Stromverbrauch mit der richtigen Frequenz schwanken zu lassen.

Das Display zeigt den momentanen Energieverbrauch eines "Smart Homes", einem vernetzten Zuhause. (Bild: dpa, Thalia Engel)

3 Angriffsszenarien

Die österreichischen Forscher schildern drei mögliche Angriffsszenarien:

1. Statische Verbrauchsattacke

Dabei wird der Stromverbrauch an vielen Verbrauchern so weit wie möglich erhöht. Kann das Netz nicht ausreichend (schnell) reagieren, muss es Teile des Netzes abschalten. Dieser Angriff ist besonders zu Zeiten erfolgversprechend, zu denen der Stromverbrauch natürlich hoch ist.

2. Dynamische Verbrauchsattacke

Der Angreifer lässt den Stromverbrauch gezielt an- und abschwellen. Das Stromnetz reagiert darauf mit der Zu- oder Abschaltung von Stromquellen, was aber immer ein bisschen dauert und zu Überschießen neigt. Der Angreifer kann mit einem simplen Messgerät an einer Steckdose die Netzfrequenz messen und schneller darauf reagieren, als die Netzregeltechnik.

Studienautor Adrian Dabrowski forscht im Bereich IT-Sicherheit (Bild: Daniel AJ Sokolov)

Bei einer schlagartigen Zunahme der Stromabnahme sinkt die Netzfrequenz unter die Norm von 50 Hz. Sobald der Stromversorger reagiert und zusätzliche Stromquellen ins Netz einspeist, steigt die Frequenz wieder. Findet der Angreifer die Eigenfrequenz der Regelkreisläufe des Stromnetzes, kann er erheblichen Schaden anrichten.

Bereits bei einer Unterschreitung der Normfrequenz (50 Hz) um nur 0,2 Hz werden im kontinentaleuropäischen Stromnetz die Pumpen von Pumpspeicherkraftwerken

abgeschaltet, bei einer Unterschreitung von 1 Hz muss der Verbrauch durch Teilnetzabschaltungen um zehn bis 15 Prozent gesenkt werden. Regionale Stromausfälle sind die Folge.

3. Zonenattacke

Hier werden gezielt Hochspannungsverbindungen zwischen Regelzonen angegriffen. Deutschland hat vier Regelzonen, Österreich und die Schweiz je eine. Ein Angreifer kann durch veröffentlichte historische Daten sowie die Beobachtung von Strombörsen abschätzen, welche Hochspannungsleitungen bereits besonders beansprucht sind.

Steuert das Botnetz den Verbrauch in zwei Regelzonen gegengleich, so dass größere Ausgleichsströme über die Hochspannungsleitungen fließen, können die Sicherungen die Leitungen trennen. Das erhöht die Last auf anderen Hochspannungsleitungen, was einen Dominoeffekt auslösen kann.

2,5 Millionen Bots könnten reichen

Wie viele Bots für einen erfolgreichen Angriff erforderlich sind, hängt von der Zusammensetzung des Botnetzes und den Sicherheitsreserven der Stromnetze ab. Simulationen der Studienautoren, Adrian Dabrowski und Johanna Ullrich, haben ergeben, dass zwischen 2,5 Millionen und 9,8 Millionen Bots ausreichen würden. Da bereits Botnetze im zweistelligen Millionenbereich gesichtet wurden, ist das kein unrealistisches Szenario.

Studienautorin Johanna Ullrich ist Ingenieurin für Elektrotechnik und Elektronik. (Bild: SBA Research)

Die Inspiration zu der Studie hat Mitautor Dabrowski aus einer Meldung des heise Newstickers über einen **Schaltsekunden-Bug im Linux-Kernel [1]**: "Der Bug hat damals den Stromverbrauch in Rechenzentren sprunghaft ansteigen lassen", schilderte der IT-Sicherheitsforscher heise online, "Da habe ich mich gefragt, ob man so etwas gezielt ausnutzen kann."

Abwehr ist teuer

Klassische Kraftwerksturbinen sind dank ihrer Schwungmasse träge, was einen gewissen Schutzeffekt gegen solche Angriffe mit sich bringt. Mit zunehmender Verbreitung von Solar- und Windkraft geht dieser Schutz aber verloren, so dass die Stromversorgung anfälliger wird.

"Grundsätzlich kann man mit Schwungrädern oder großen Akkus helfen, solche Attacken zu erschweren", sagte Elektrotechnik-Ingenieurin Ullrich, "Aber es müsste erst erforscht werden, welcher Aufwand dafür in der Praxis notwendig wäre." Ein weiterer Ansatz seien **"smarte" Stromnetze [2]**, die von sich aus vernetzte Verbraucher steuern können – das Gegenstück zum Botnetz also.

Diese smarten Netze gibt es im Unterschied zu Botnetzen aber noch nicht. Außerdem wäre ihr Effekt im konkreten Szenario beschränkt. Während Akku-Ladegeräte oder Wasserboiler durchaus in sehr kurzen Intervallen ein- und ausgeschaltet werden könnten, wäre das bei Waschmaschinen oder Kühlgeräten nicht praktikabel. Und Dabrowski warnt vor einer neuen Gefahrenquelle: "Erlangt ein Angreifer die Kontrolle über ein solches smartes Stromnetz, wird der Bock zum Gärtner."

- Das Paper heißt "**Grid Shock: Coordinated Load-Change Attacks on Power Grids [3]**" und wurde Anfang Dezember auf der Annual Computer Security Applications Conference (ACSAC 2017) auf Puerto Rico vorgestellt.

(**ds [4]**)

URL dieses Artikels:
`http://www.heise.de/-3927886`

Links in diesem Artikel:
`[1]` https://www.heise.de/meldung/Schaltsekunden-Bug-in-Linux-verschwendet-Strom-1631325.html
`[2]` https://www.heise.de/thema/Smart-Grid
`[3]` https://www.sba-research.org/wp-content/uploads/publications/201712%20-%20ADabrowski%20-%20Grid%20Shock.pdf
`[4]` mailto:ds@heise.de